On a Conjecture of Erdös and Rényi*

Ki Hang Kim and Fred W. Roush
Mathematics Research Group
Alabama State University
Montgomery, Alabama 36101

Submitted by Richard A. Brualdi

ABSTRACT

We show that for A ranging over $n \times n$ circulants with three ones in each row, where n is prime, $\liminf |\det A|^{1/n} > 1$. For a subfamily containing almost all A's this liminf is in fact 1.38.... We also compute the permanents of a certain family of matrices.

1. INTRODUCTION

Let $S_n(k,k)$ denote the set of all $n \times n$ $(0,1)$-matrices each of whose row sums and column sums is k. Erdös and Rényi [2] have conjectured that

$$\liminf (\operatorname{per} A)^{1/n} > 1$$

for $A \in S_n(k,k)$ with fixed $k \geqslant 3$. This paper is an attempt to provide information on this question. Some related work was done in [1], [3], and [4].

Erdös and Rényi's conjecture is a sort of *weakened form of the van der Waerden conjecture* that $\operatorname{per} B \geqslant n!/n^n$ for all doubly stochastic matrices B. In fact if the van der Waerden conjecture holds, then

$$(\operatorname{per} A)^{1/n} \geqslant (n!)^{1/n}(k/n).$$

We show that for A ranging over circulants in $S_n(3,3)$, and n *restricted to primes*,

$$\liminf |\det A|^{1/n} > 1.$$

*This work was supported by Alabama State University Faculty Research Grant R-78-6.

 0024-3795/79/010179+11 $01.75

In the process we prove that for almost all circulants of this type

$$|\det A|^{1/n} \to 1.38135\ldots$$

as n tends to infinity over primes.

Then we show that for certain families of non-circulants [not in $S_n(3,3)$],

$$\lim_{n->\infty} (\operatorname{per} A)^{1/n}$$

can be made arbitrarily close to 1.

2. DETERMINANTS OF CIRCULANTS

Let P be the $n \times n$ permutation matrix with ones in all locations $(i, i+1)$ modulo n. Then by multiplying by a power of P, any circulant in $S_n(3,3)$ can be reduced to the form $I + P^a + P^b$ for some a, b. If n is prime, such a circulant can further be reduced to the form $I + P + P^k$ by conjugating by permutation matrix Q, where $q_{ij} = 1$ iff $aj \equiv i \pmod{n}$. We have

$$\operatorname{per}(I + P^a + P^b) \geqslant |\det(\pm I \pm P^a + P^b)|.$$

The eigenvalues of P are $1, \xi, \xi^2, \ldots, \xi^{n-1}$, where ξ is a primitive nth root of unity. Thus

$$\det(\pm I \pm P^a + P^b) = \prod_{j=1}^{n} (\pm 1 \pm \xi^{aj} + \xi^{bj}).$$

PROPOSITION 1. *Let Θ_i for $i = 1$ to b be the roots of $y^a + \delta_1 y^a + \delta_2 = 0$, where $\delta_i = \pm 1$. Then*

$$|\det(P^b + \delta_1 P^a + \delta_2)| = \prod_{i=1}^{b} |\Theta_i^n - 1|.$$

Proof. We write $\xi^{bj} \pm \xi^{aj} \pm 1$ as

$$\prod_{i=1}^{b} (\xi^j - \Theta_i).$$

Then the product of all the $\xi^{bj} \pm \xi^{aj} \pm 1$ is a product of terms of the form

$$(-1)^n \prod_{j=1}^{n} (\Theta_i - \xi^j) = (-1)^n(\Theta_i^n - 1). \qquad \blacksquare$$

COROLLARY 2. *If we fix a,b and let n increase,*

$$\left|\det\left(P^b + \delta_1 P^a + \delta_2\right)\right|^{1/n}$$

approaches the product of all the $|\Theta_i|$ which are >1 if we exclude values of n such that an nth root of unity occurs among Θ_i.

Proof. If $|\Theta_i| > 1$, $|\Theta_i^n - 1|^{1/n}$ approaches $|\Theta_i|$. If $|\Theta_i| < 1$, $|\Theta_i^n - 1|^{1/n}$ approaches 1. Suppose $|\Theta_i| = 1$. Then for Θ_i,

$$1 = |y^b| = |1 \pm y^a| = 2 \pm 2\cos au,$$

where $y = e^{iu}$. Therefore $y^a = \pm e^{\pm 2\pi/3}$. Therefore y is a root of unity of order at most $6a$, and $|\Theta_i^n - 1|^{1/n}$ will approach 1 excluding cases when $\Theta_i^n = 1$. $\blacksquare$

LEMMA 3. *Let a and b be positive integers, and let $c = a/(a,b)$ and $d = b/(a,b)$. A root of unity will occur among the roots of $y^b + (-1)^{e+f} y^a + (-1)^f$ iff $c - 2d \equiv 0 \pmod 3$, $c \not\equiv 0 \pmod 3$, $d \not\equiv 0 \pmod 3$, and either $c \equiv e \pmod 2$ and $d \equiv \pmod 2$ or $e \equiv f \equiv 0 \pmod 2$.*

Proof. A root of unity occurs among the roots of the given equation iff one occurs among the roots of $y^d + (-1)^{e+f} y^c + (-1)^f$. As in the proof of Corollary 2, $y^c = (-1)^e \omega$ where ω is a primitive cube root of unity. Then $y^d = (-1)^f(-\omega - 1) = (-1)^f \omega^2$.

Since $(c,d) = 1$, $y = y^{rc+sd}$ for some r,s. Therefore $y = (-1)^k \omega^j$ for some k,j. Substituting this into the equations for y^c and y^d, we obtain the equations of the lemma. $\blacksquare$

LEMMA 4. *For $0 \leqslant x \leqslant \pi/2$, $1 + \sqrt{3}\, e^{ix}$ has the form $re^{i\Theta}$ for $r > 0$, $0 \leqslant \Theta \leqslant 2x/3$.*

Proof. This amounts to

$$\arctan \frac{\sqrt{3}\, \sin x}{1 + \sqrt{3}\, \cos x} \leqslant \tfrac{2}{3} x.$$

This inequality is true at $x=\pi/2$ and $x=0$ and at the only critical point of the difference function, $\arccos(1/\sqrt{3})$, in the interval. ■

LEMMA 5. *Let u be a number of the form*

$$\frac{2k\pi - e\pi}{2b-a}$$

such that $bu \equiv (f+1)+z/2 \pmod{2\pi}$, where $0 \leqslant x \leqslant 4\pi/9$. Let R_u be the set of complex numbers $re^{i\Theta}$ such that

$$1 \leqslant r \leqslant 3^{1/b}, \qquad u \leqslant \Theta \leqslant u + \frac{x}{6b-4a}.$$

Then if $b \geqslant 2a$, the equation

$$y^b + (-1)^{e+f} y^a + (-1)^f$$

has a root in the set R_u.

Proof. Let $f(z) = -z^b$ and $g(z) = (-1)^{e+f} z^a + (-1)^f$. We will show $f(R_u) \supseteq g(R_u)$ and apply a fixed point theorem.

From the definition of u it follows that $2bu \equiv au + e\pi \pmod{2\pi}$. Therefore the function $(-1)^{e+f} z^a$ will send R_u to the set R' given by $1 \leqslant r \leqslant 3^{a/b} \leqslant \sqrt{3}$, $f\pi + x \leqslant \Theta \leqslant f\pi + x + ax/(6b-4a)$. We have

$$x + \frac{ax}{6b-4a} \leqslant x\left(1 + \frac{a}{8a}\right) \leqslant \frac{\pi}{2}.$$

Therefore for $z \in R'$, $|(-1)^f + z| \geqslant \sqrt{2} > 1$. Also it is true that $|(-1)^f + z| = 1 + \sqrt{3} < 3$. We may determine the extremes on the angles of $(-1)^f + z$ by considering the points $\exp(f\pi i + xi)$ and $\sqrt{3}\exp[f\pi i + axi/(6b-4a)]$. The former will go to a point at an angle of $f\pi + x/2$, and the latter will go to a point at an angle less than or equal to

$$f\pi + \frac{2}{3}\left(x + \frac{ax}{6b-4a}\right)$$

by Lemma 4. But

$$\frac{2}{3}\left(x + \frac{ax}{6b-4a}\right) = \frac{x}{2} + \frac{bx}{6b-4a}.$$

Therefore $g(R_u) \subseteq f(R_u)$. Both f,g are 1-1 on R_u. Therefore $f^{-1}g$ is a well-defined continuous function from R_u to itself. It will have a fixed point z_0 which will be a root of $y^b + (-1)^{e+f} y^a + (-1)^f$. This completes the proof. ■

THEOREM 6. *Let a and b be positive integers and $a < b$. There exists a constant $c > 1$ such that for every a,b we can choose e,f such that*

$$\liminf |\det[P^b + (-)^{e+f} P^a + (-)^f]|^{1/n} \geqslant c.$$

Proof. By Lemma 3 we can choose e,f so that the determinant is non-zero for every n. Then the liminf will be the product of the absolute values of all roots of $y^b(-1)^{e+f} y^a + (-1)^f$ which have absolute values larger than 1, by Corollary 2. This product will be the same for mb, ma as for b,a if m is an integer. Therefore we may assume $(b,a) = 1$. Also it will be the same for b,a as for $b, b-a$, since this change is equivalent to replacing y by $1/y$, and the product of the absolute values of all roots of the equation is 1. All roots of the type given by Lemma 5, and their conjugates, will have absolute value at least $2^{1/2b}$, since the angle between $(-1)^f$ and $(-1)^{e+f} y^a$ was shown to be at most $\pi/2$. There will be $2b-a$ distinct numbers of the form

$$\frac{2k\pi - e\pi}{2b-a},$$

and if $(b,a) = 1$, the multiples by b of these numbers will be distinct and equally spaced around the circle. The inequality on bu means in effect that bu must lie in a certain $\frac{1}{9}$ of circle. Therefore $\frac{1}{9}(2b-a) - 1$ values of u give rise to roots of the equation. Another $\frac{1}{9}(2b-a) - 1$ roots are given by the conjugates of these roots. Thus there are at least $\frac{2}{9}(3b/2) - 2$ roots of the equation with absolute value at least $2^{1/2b}$. This gives a constant c for all values of $b > 6$. The inf of this c and the values of the limit for the finite set of pairs $\{a,b\}$ with $a \leqslant b \leqslant 6$ give a c valid for every a,b. ■

Since we only used e,f to ensure the determinant was non-zero, we also have:

THEOREM 6*. *Let a and b be positive integers and $a < b$. There exists a constant $c > 1$ such that for any a,b*

$$\liminf |\det(I + P^a + P^b)|^{1/n} > c$$

if the liminf *is taken over prime values of n only.*

3. GEOMETRIC MEANS

THEOREM 7. *Let $u(n)$ tend to infinity with n, where n ranges over prime numbers. Let $k(n)$ be a sequence of integers such that $k(n) \not\equiv ab^{-1} \pmod{n}$ for any a, b with $|a|, |b| < u(n)$. Then*

$$\log(|\det(I + P + P^{k(n)})|^{1/n})$$

approaches

$$\frac{1}{2\pi}\int_0^{2\pi/3} \log(2 + 2\cos\theta)\, d\Theta$$

as n tends to infinity over prime numbers.

Proof. We first show that the pairs $(j, kj) \bmod n$ are uniformly distributed in a certain sense. Let $f(x, y)$ be any continuous function of two variables on the unit circle. Let ξ be $e^{2\pi i/n}$. Then

$$\frac{1}{n}\sum_{j=0}^{n-1} f(\xi^j, \xi^{kj}) \to \frac{1}{4\pi^2}\int\int f(x, y)\, dx\, dy.$$

By the Weierstrass theorem it is only necessary to verify this result for $f(x, y) = x^a y^b$. But for any fixed a, b, not both zero,

$$\frac{1}{n}\sum_{j=0}^{n-1} \xi^{j(a+kb)} = 0$$

whenever n is large enough that k cannot be represented as $-a/b$. This agrees with

$$\left(\frac{1}{2\pi}\right)^2 \int e^{ai\Theta} e^{bi\psi}\, d\Theta\, d\psi.$$

Likewise we have equality when $a = b = 0$. This proves the uniform distribution.

The function we are interested in, $\log|1 + x + y|$, fails to be continuous at the points $(e^{2\pi i/3}, e^{4\pi i/3})$ and $(e^{4\pi i/3}, e^{2\pi i/3})$. However, the result does hold for all the continuous functions $\sup\{\log|1 + x + y|, \alpha\}$ for $\alpha \in \mathbf{R}$, and we will show these can be used instead.

Consider the set T of j such that $|j|<[n/2]$ and $|1+\xi^j+\xi^{kj}|<\delta$. On this set $-\delta<|1+\xi^j|-1<\delta$, so $|2\cos(\pi j/n)-1|<\delta$. If $\delta<\frac{1}{10}$, the mean value theorem implies

$$2\cos(\pi j/n) = 1+\left(\frac{2\pi j}{n}-\frac{2\pi}{3}\right)x, \qquad 0.8 < x < 1,$$

for $2\pi j/n$ near $2\pi/3$, and a similar result near $-2\pi/3$.

If n is a prime >3, $|2\pi j/n-2\pi/3|$ must be at least $2\pi/3n$. By essentially the same argument as above we have $|1+\xi^j+\xi^{kj}| \geqslant |2\cos(\pi j/n)-1|$. Therefore

$$\prod |1+\xi^j+\xi^{kj}|^{1/n},$$

taken over j in the set T, is greater than or equal to

$$\left\{\left(\frac{2\pi}{3n}\,\frac{4}{5}\,\frac{8\pi}{3n}\,\frac{4}{5}\cdots\frac{2\pi+6s\pi}{3n}\,\frac{4}{5}\right)^{1/n}\right\}^4$$

(The fourth power is from the fact that T consists of four parts.) Here $s=[(15n\delta/24\pi)-\frac{1}{3}]$. This expression is greater than or equal to

$$\left(\frac{8\pi}{15}\right)^{4(s+1)/n}\frac{\{(s+1)!\}^{4/n}}{n^{4(s+1)/n}} \geqslant C_1^{\delta}\delta^{4\delta}$$

for a constant C_1 independent of all choices. And $\prod|1+\xi^j+\xi^{kj}|^{1/n}$ for $j\in T$ is less than 1. Thus

$$\begin{aligned}\left|\frac{1}{n}\sum \sup\{f,\log\delta\}-\frac{1}{n}\sum f\right| &\\ \leqslant \frac{|T|}{n}|\log\delta| + 4\delta|\log\delta| + \delta|\log C_1| &\\ \leqslant C_2\delta|\log\delta| + \delta|\log C_1|, & \qquad (1)\end{aligned}$$

where C_2 is a constant independent of all choices. Thus if $\delta\to 0$ with n, this difference will tend to zero.

Now we use the same approach to the integral. Let T_1 be the set of θ,ψ such that $|1+e^{i\theta}+e^{i\psi}|<\delta$. We have $|1+e^{i\theta}+e^{i\psi}| \geqslant \max\{|2\cos(\theta/2)-$

$1|, |2\cos(\psi/2)-1|\}$. So T_1 is contained in the set $T_2=\{\theta,\psi: |2\cos(\theta/2)-1|<\delta,\ |2\cos(\psi/2)-1|<\delta\}$.

$$\int_{T_2} \log|1+e^{i\theta}+e^{i\psi}|\,d\theta\,d\psi$$

$$\geqslant \int_{T_2} \log|2\cos(\theta/2)-1|\,d\theta\,d\psi$$

$$\geqslant 16\int_{2\pi/3}^{2\pi/3+5\pi/4}\int_{2\pi/3}^{2\pi/3+5\pi/4} \log\frac{4}{5}\left(\theta-\frac{2\pi}{3}\right)d\theta\,d\psi$$

$$\geqslant 16\left(\tfrac{5}{4}\right)^2(\log\delta-1).$$

This shows

$$\frac{1}{4\pi^2}\int f\,dx\,dy$$

is defined as a Cauchy principal value, and

$$\frac{1}{4\pi^2}\int \sup\{f,\log\delta\}\,dx\,dy-\frac{1}{4\pi^2}\int f\,dx\,dy \leqslant C_3\delta\log\delta \tag{2}$$

for a constant C_3 independent of all choices.

From (1) and (2) and the uniform distribution of (i,ki) mod n it follows that

$$\frac{1}{n}\sum \log|1+\xi^i+\xi^{ki}| \to \frac{1}{4\pi^2}\int f\,dx\,dy$$

for every value of k satisfying the hypothesis of the theorem.

Then an evaluation of

$$\frac{1}{4\pi^2}\int \log(1+e^{i\theta}+e^{i\psi})\,d\theta\,d\psi$$

proves the theorem. ■

4. ERDÖS-RÉNYI CONJECTURE

THEOREM 8. *There exists a constant $d>1$ such that if n is prime, $n>3$, then*

$$|\det X|^{1/n} > d$$

for all $n\times n$ circulant X whose row sums are three.

Proof. For any positive integer p and positive real number r there exists a positive integer $\#(p,r)$ such that for $n \geqslant \#(p,r)$ and $p>b>a>0$ and $(b,a)=1$,

$$\left| \left| \prod (\theta_i^n - 1) \right|^{1/n} - \prod_{|\theta_i|>1} |\theta_i| \right| < r.$$

This is true because for any fixed a,b with $b>a>0$ and $(a,b)=1$ the expression on the left tends to zero. [For $(a,b)=1$ there are at most two θ_i such that $|\theta_i|=1$, and these will be cube roots of unity].

Take $r=(c-1)/2$ for c as in Theorem 6*. Then for a circulant $I+P+P^k$, $1<k<n$, suppose k can be represented as $\pm ba^{-1} \pmod n$ with $b \geqslant a>0$ such that $n>\#(2p,r)$. Then it can be represented in this form with $b>a>0$ and $(b,a)=1$ unless $k=-1$, in which case we can replace the circulant with $I+P+P^2$. Then we can replace the circulant with a circulant $I+P^{a(1)}+P^{b(1)}$, where $b(1)>a(1)>0$, $(b(1),a(1))=1$ and $b(1)\leqslant 2b$. It follows from Theorem 6* that

$$\prod_{|\theta_i|>1} |\theta_i| > c.$$

Therefore

$$\left| \prod (\theta_i^n - 1) \right|^{1/n} > 1 + r.$$

So with $d=1+r$ the theorem holds in this case.

Other values of k will be treated by Theorem 7 with $u(n)$ the largest number b such that $\#(2b,r)<n$, or 1 if no such b exists. This sequence will tend to infinity. For any sequence of such numbers k,

$$|\det(I+P+P^k)|^{1/n}$$

will converge to 1.38....

Therefore there must be a lower bound on

$$|\det(I+P+P^k)|^{1/n}.$$

With d equal to this bound the theorem holds in the present case. This proves the theorem. ■

5. AN EXAMPLE

THEOREM 9. *For fixed k let X_n be the matrix which has ones exactly in those locations i,j such that $i=j$, $i=j+1$, or $i+k=j$. Then the permanent of X_n satisfies the recursion formula*

$$\operatorname{per} X_n = \operatorname{per} X_{n-1} + \operatorname{per} X_{n-k-1}.$$

Let Y_n be the matrix obtained from X_n by adding a 1 entry in location $(1,n)$. Then

$$\operatorname{per} Y_n = 1 + \operatorname{per} X_n.$$

Proof. Expand $\operatorname{per} X_n$ by minors on the first column. The first minor gives $\operatorname{per} X_{n-1}$. The second gives the permanent of a matrix for which any non-zero diagonal in the first k columns must pass through $(2,1),(3,2),\ldots,(1,k)$. When the rows and columns of all these entries have been deleted, the matrix X_{n-k-1} is obtained.

It can be seen that exactly one generalized diagonal passes through $(1,n)$-entry in Y_n. This proves the second formula. ■

COROLLARY 10. *Let r_0 be the largest root of $x^{k+1}-x^k-1$. Then*

$$\lim_{n->\infty} (\operatorname{per} X_n)^{1/n} = \lim_{n->\infty} (Y_n)^{1/n} = r_0.$$

REMARK. This implies for instance that we can take a circulant with row sums equal to 3, change 30 consecutive ones on the main diagonal to zero, and have a matrix Y with

$$(\operatorname{per} Y)^{1/n} < 1.088 < 3/e$$

of arbitrarily large size.

COROLLARY 11. *By choosing k large,*

$$\lim_{n\to\infty} (\operatorname{per} X_n)^{1/n}$$

can be made arbitrarily close to 1. *In fact*

$$\lim_{n\to\infty} (\operatorname{per} X_n)^{1/n} \leqslant \left(1-\frac{\log(k+1)}{k+1}\right)^{-1}.$$

Proof. By Corollary 10, this limit will be the largest real root of $y^{k+1}=y^k+1$. Let $z=1/y$, so that $1=z+z^{k+1}$. But

$$\left(1-\frac{\log(k+1)}{k+1}\right)^{k+1} < \frac{\log(k+1)}{k+1}$$

can be shown by taking logarithms of both sides and expanding the left hand side in the power series for $\log(1-x)$. Therefore

$$z > 1-\frac{\log(k+1)}{k+1}.$$

This proves the corollary. ■

The authors would like to thank Richard Brualdi, Edward Wang, and an unknown referee for very constructive criticism of the manuscript.

REFERENCES

1 R. A. Brualdi and M. Newman, Some theorems on permanents, *J. Res. Nat. Bur. Standards Sect. B*, 69B-3:159–163 (1965).
2 P. Erdös and A. Rényi, On random matrices II, *Studia Sci. Math. Hungary.*, 3:459–464 (1968).
3 H. Minc, Permanents of (0, 1)-circulants, *Canad. Math. Bull.*, 7:253–264 (1964).
4 H. Minc, On permanents of circulants, *Pacific J. Math.*, 42:477–484 (1972).

Received June 1977; revised 19 December 1977